

Lenovo AI Readiness Index Series 2025

Unleash AI with total security.

How to ensure your AI is trusted and
secure—so you innovate with confidence.

Smarter
technology
for all

Lenovo

Unleash AI with less risk.

Security is a priority for enterprises, but many still struggle with data protection and compliance risks.

With its potential to deliver operational efficiency, smarter decision-making and drive innovation, AI is fast becoming a business essential. However, organizations are aware of the potential cyber threats and data privacy posed by AI and recognize the need to mitigate these risks before, during and after adoption.

It’s something leaders take seriously. Security and privacy for AI is ranked in the top 5 AI investments for the next 12 months, according to the Lenovo/IDC CIO Playbook 2025. Lenovo’s latest research reveals that confidence in AI security readiness is generally high. But there are still issues—particularly the risk of exposing business IP or customer data.

These issues are highlighted in the Lenovo AI Readiness Index Series 2025, our global benchmarking survey of 5,000 senior business leaders and in-depth interviews with 40 global business and IT leaders across 20 countries. The survey assesses their AI readiness across four pillars: technology, process, people and security.

In this report, we explore the security pillar, revealing key challenges from risk mitigation and vetting third parties to data protection. All these issues can slow down AI time to value. Here, we dive into how leaders are addressing them, showing you how you can realize AI value faster—today and tomorrow.

Stand-out findings.

- 1

Businesses struggle with risk mitigation.
The extent to which AI projects fully mitigate security risks and other unintended consequences was one of the weakest areas in the entire AI Readiness Index study, with almost one in five businesses (18%) having low or very low confidence.
- 2

Managing risk is slowing AI innovation.
Constant change due to evolving threats and regulation adds cost and slows time to value. While businesses are taking steps to protect themselves, major concerns remain—particularly in vetting and managing third-party suppliers, with 48% of executives mentioning this in interviews. Data protection is also a top priority—63% of interviewees mentioned protecting customer data and 49% cited protecting company data.

Contents.

Click to explore how to minimize risk in your AI:

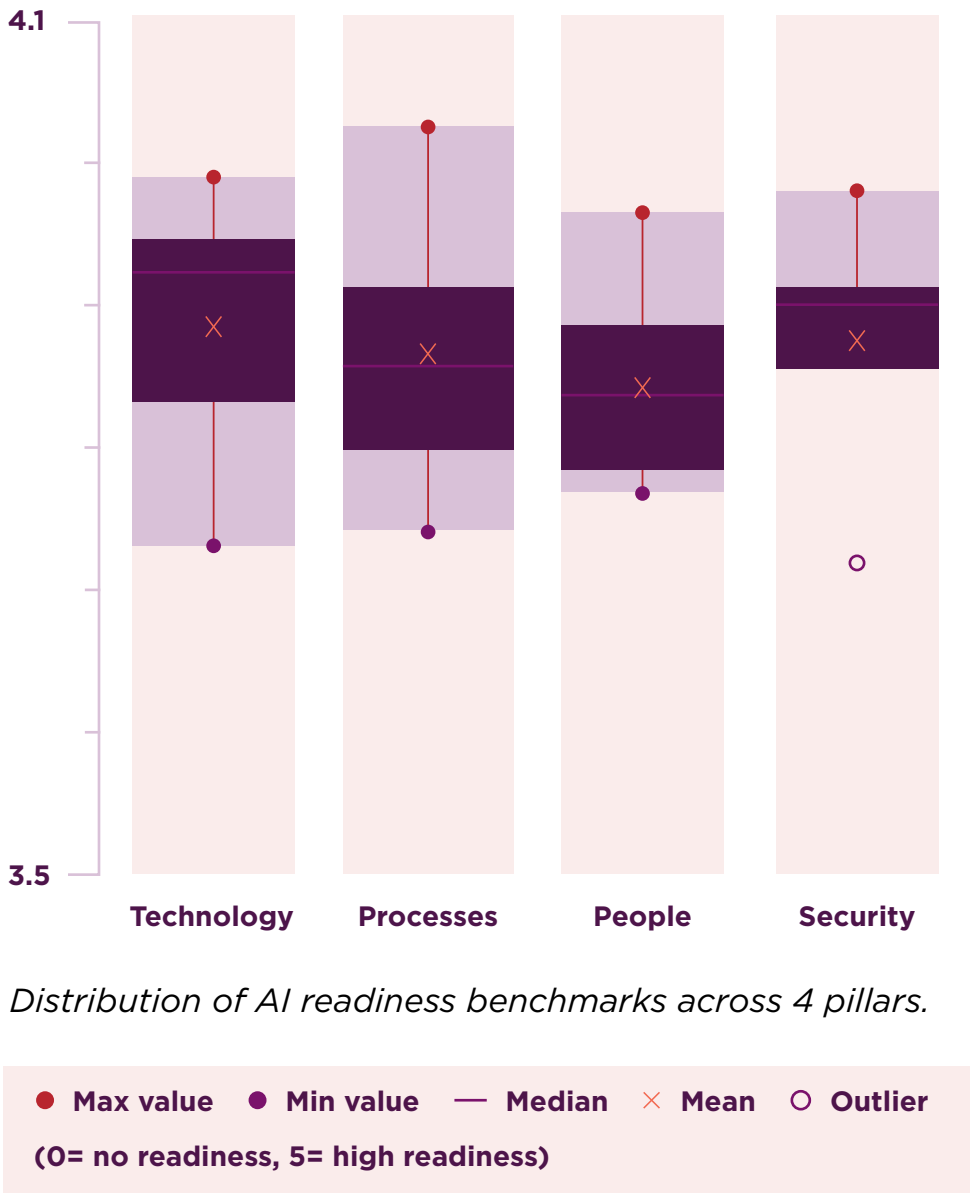


Security AI readiness summary

Optimism and risk awareness remain high.

Enterprises are broadly confident in their AI security but are vigilant about rising threats.

Security is one pillar of Lenovo’s AI Readiness Assessment, sitting alongside people, technology and process as the key components to successful AI implementation.



Security has the highest mean benchmark score across the four pillars—followed closely by technology (see chart above).

Even so, there are some potential vulnerabilities that could leave organizations exposed as they scale AI initiatives. These include an increased surface area for cyber attacks or breaches and the risk of exposing data or IP to competitors.

Clearly, building trust in the security of your AI deployment is essential for an optimized investment. Any concerns will hold people back from using AI to its full potential

Strong data governance can also be the difference between a successful AI project and an unsuccessful one. According to the Lenovo/IDC CIO Playbook 2025, poor data quality is the number one reason AI projects fail¹. You need clear policies on data accuracy, security and accessibility, as well as AI models that are explainable and compliant.

“

AI is 100% trust-based. If you and your team don’t trust AI is working for your benefit and working for good—i.e. maintaining data in a way it should be maintained—then your project is finished.”



Rick Kreuser,
Director, AI Portfolio,
Lenovo



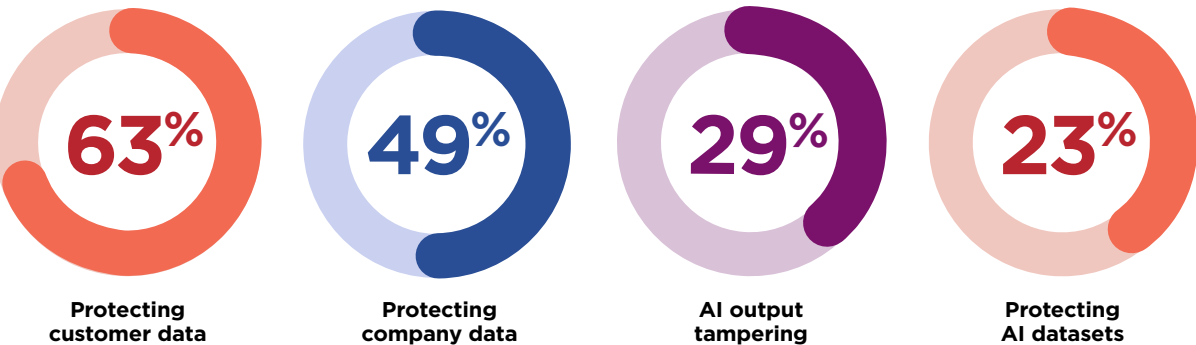
Understanding AI risks.

Being confident doesn't mean being safe.

Our respondents claim to have strong AI readiness in security-related areas. Indeed, 71% reported high or very high confidence in effectively monitoring and managing security breaches enabled by AI.

However, our research indicates that companies do know what's at stake. When asked in interviews about the security challenges that emerged as they attempted to integrate AI into their systems, executives' responses were wide ranging.

Frequency of mentions in 40 executive interviews.



Protecting customer and company data are the top security challenges surrounding AI.

“

Cyber attacks, data breaches, adversarial model manipulation, insider threats, compromised IoT devices, and supply chain vulnerabilities have all contributed to heightened skepticism regarding AI's capabilities.

This skepticism led us to closely monitor AI operations.”

**C-level legal executive,
Hospitality business, Brazil**

But what exactly is the security challenge? Our research revealed four key AI risks that must be addressed. Left unchecked, organizations and their sensitive data can be left exposed.

Top AI risks.

Click to jump to each section:

-
-
-
-
-
-



1

Increasing points of attacks.

As data spreads further, more access points are exposed.

AI expands how far data can spread within an organization—and beyond. AI is often connected to a network of systems and devices or third-party providers, increasing the number of potential access points.



businesses reported low or very low preparedness for monitoring and managing security breaches enabled by AI.

Retail was the sector suffering most, with one in eight businesses (13%) reporting low or very low readiness for managing security breaches. As retailers manage high volumes of traffic, transactions, users and partners in the supply chain, the security landscape can become complex. Given the further challenge of frequently fluctuating cashflows, retailers need to select their investments wisely.

What executives are saying.

Organizations worry about vulnerabilities increasing as they migrate data to new AI tools.

“

Previously we were using mainframes to store critical data, but mainframes were not capable of fully integrating AI or new tech into it, so we shifted to the cloud, and this has made us vulnerable to cyber attacks and data breaches.”

CIO, Retail business, UK

“

Connecting AI tools to older manufacturing systems has increased the risk of exposing sensitive operational data to cyber attacks. As AI models depend on large datasets, protecting these datasets during transfer and storage is challenging, especially against data breaches or unauthorized access.”

VP Operations, Manufacturing business, Argentina

Considerations for leaders.

Double down on your controls—for both the way in and way out. This means controlling both access to the users prompting the AI and what data is shared on the way out, so people only get access to the information they’re meant to see.

2

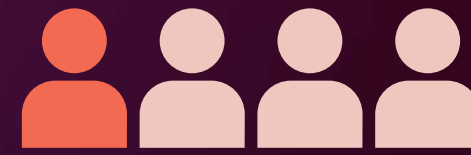
Supply chain exposure.

It only takes one weak link to compromise an entire supply chain.

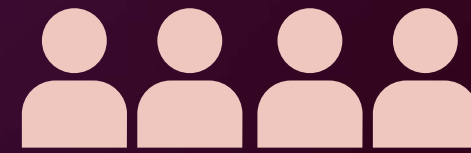
AI can revolutionize supply chains—improving efficiency, decision-making, forecasting and more.

However, it also exposes organizations to greater risks. The third-party data, models and algorithms on which organizations rely may contain vulnerabilities, biases or malicious code. If an upstream vendor's AI systems are compromised, they can cascade security and operational risks.

Upstream systems can also include your business' own internal systems. For instance, if your permissions to access data in your ERP system aren't correct, a chatbot or agent may gain access to unauthorized data. This is especially true where there's unstructured data, which are notorious for lack of controls.



1 in 8



businesses (12%) have low or very low confidence in having adequate policies and processes in place to identify AI supply chain risks.

What executives are saying.

Organizations are adopting comprehensive vetting processes.

“

We rely on external partners for AI tools and platforms, which can introduce risks related to intellectual property theft and supply chain disruptions. To mitigate these risks, we are adopting a more rigorous vetting process for third-party vendors and making sure that they adhere to high-security standards, have proven track records in data protection, and establish a clear contractual agreement that outlines security responsibilities and liabilities that can help safeguard us against potential breaches.”

C-level legal, Hospitality business, Brazil

Considerations for leaders.

Establish a robust supply chain assessment with monitoring and mitigation capability that's informed by your business' risk appetite.

Consider using a single partner's solution. NVIDIA NIM, for example, comprises technology by multiple vendors behind the scenes, but is certified as being secure throughout the supply chain.

3

More sophisticated data threats.

Executives fear attackers will target AI datasets with tougher-to-spot techniques.

Centralized AI datasets are an attractive target for phishing or ransomware attacks due to the comprehensive volume of information that could be exploited.

Executives fear data used to train AI is open to potential manipulation—such as data poisoning or prompt injections—or adversarial AI, where attackers create inputs designed to deceive AI models.

Another concern is that increased autonomy provided by Agentic AI could result in a lack of transparency, making it more difficult to understand where data has come from and how it has been manipulated.

What executives are saying.

Organizations are concerned about the wide range of attacks and their potential consequences.

“

Phishing attacks were the primary security challenge we faced as we attempted to integrate AI. The attackers could use various methods to compromise the data and security of a supplier through phishing emails. If the attackers could access our systems, they could steal sensitive information and disturb the whole operation of the company.”

**VP Operations,
Oil and gas business, USA**

AI sabotage is another serious concern for interviewees.

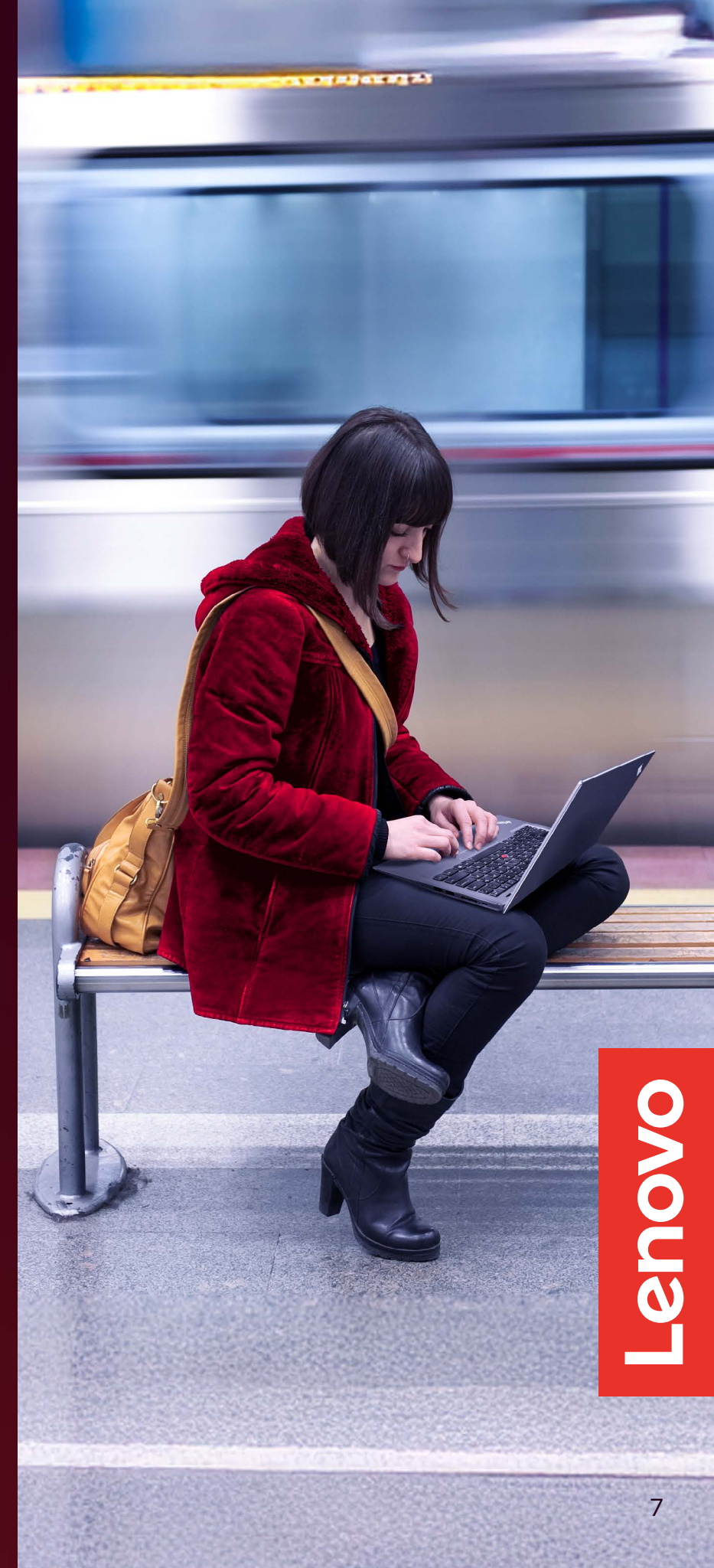
“

Data poisoning was a major challenge we faced in terms of security in AI. This is a cyber attack which somehow gets into your systems and misleads inputs to AI, forcing the AI model to give false or misleading data or information.”

**IT Director,
Retail business, USA**

Considerations for leaders.

Combine rigorous education and awareness with solid security fundamentals, including a layered Defense in Depth strategy. Investigate how you can use AI to help with log scans, alerts and agents as a way to implement real-time remediation of attacks from adversarial AI.



4

IP exposure to competitors.

High-value data in potentially unsecure AI systems creates a perfect storm for damaging leaks.

Given the value tied up in data, there is a strong risk that proprietary company information could be exposed to competitors through data harvesting, leakage or unauthorized access.

For example, there have been cases where companies have banned Gen AI tools like ChatGPT after sensitive information was uploaded and put in the public domain.

There are two parts to this risk: the way some Gen AI tools absorb sensitive information and use it to form future responses to unauthorized viewers; and the people using the tools. People may not understand the sensitivity of information or the guardrails to operate within.

“

90% of the security issues you have are from people, either people intentionally or unintentionally doing something, whether it's spilling IP or being a bad actor internally or unknowingly feeding it something they shouldn't.”



Rick Kreuser,
Director, AI Portfolio, Lenovo

Considerations for leaders.

Your first line of defense should always be awareness and education. Most IP leakage occurs because users either didn't know—or didn't care—where their data was going.

Many companies will deny access to a public Large Language Model until there's a signed Master Service Agreement (MSA) governing where the data goes, its use (such as training and model improvement) and who owns it or can reuse it.

“

We were aware of the vulnerabilities in AI algorithms, which include internal risks such as the potential disclosure of data to competitors and privacy concerns regarding personal information. These were major issues that worried us.”

VP Operations,
Manufacturing business, Australia

Reducing AI risks with confidence.

Businesses need to build risk mitigation into design and management.

Our research says one of the weakest areas of AI readiness is the extent to which AI projects are designed and managed to mitigate risk and unintended consequences.



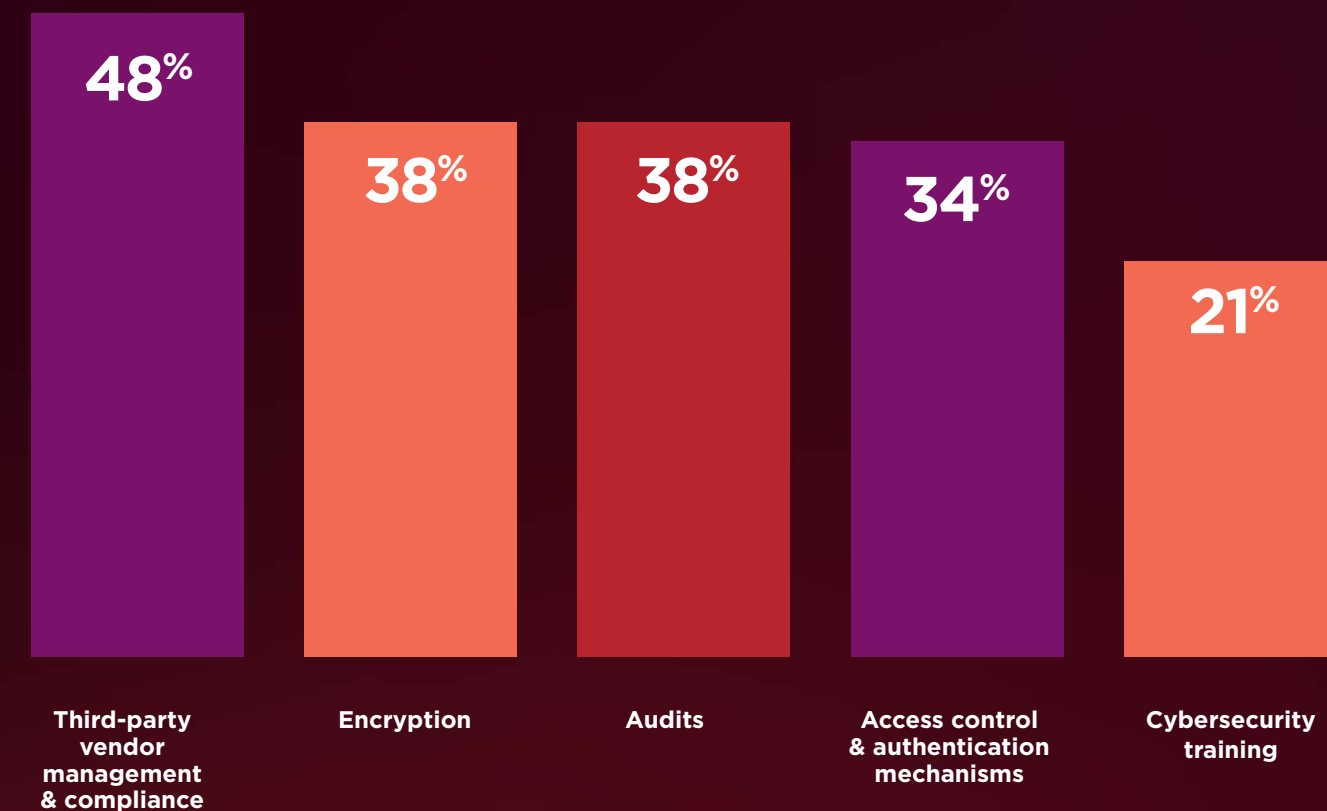
Almost 1 in 5 businesses (18%) have low or very low confidence in their ability to mitigate security risks and other unintended consequences in AI projects—one of the lowest levels of confidence reported in our survey.

At a sector level, retail and hospitality businesses struggled most. Almost one in four (22%) reported low or very low readiness.

Risk mitigation was also the area with the widest gap in confidence levels between technical and non-technical roles. While 15% of IT audiences had low or very low confidence, the figure was 21% for other business functions (such as sales, marketing and legal).

So what are organizations doing to mitigate risk while implementing AI?

Top 5 steps being taken to overcome AI security challenges.



Frequency of mentions in 40 executive interviews.

Next, we dive into detail on each of these five steps to break down what organizations are doing to ensure their security is AI-ready.


Reducing AI risks with confidence

Vet third-party suppliers.

Why it's critical and what to look out for.

Organizations need to rigorously vet third-party suppliers. It's the most common mitigation strategy identified in our research.

Previously, traditional enterprise systems were secure and standardized, with clear breach recourse due to single-entity management. But now, Gen AI solutions involve multiple, often new and uncoordinated companies, which can increase security risks.








**48%**

Nearly half of executives mentioned rigorously vetting third-party suppliers in interviews.

Confidence in policies and processes to identify if supply chain risks are adequate is a challenge for nearly one in eight respondents (12%), rising to 14% in North America and 16% in Latin America. At a sector level, retail and hospitality were most likely to report low or very low confidence (14% and 16% respectively).

So, what should you look at when assessing third-party suppliers? Focus on what could threaten your specific risk tolerances the most.

This could include:

- | | |
|--|---|
|  Corporate health |  Development processes |
|  SLA performance |  Standards |
|  Release frequency |  Transparency on vulnerability disclosure |
|  Stance on vetting their own third parties |  Commitment to vulnerability fix |
|  Results from code scans and pen tests | |

What executives are doing.

Interviews revealed that organizations follow strict vetting procedures of vendors.

“We ask vendors to give us clear information on how their AI tools manage data and regularly review third-party systems.

We also test AI tools in safe environments before fully launching them, which helps us reduce risks from weaknesses or issues related to intellectual property.”

**CFO,
Financial Services business, India**



Reducing AI risks with confidence

Add data protection.

Using AI for threat detection requires a risk-forward approach.

To protect data, businesses run encryption, multi-level fire walls and real-time monitoring. This was number two in our top five steps highlighted in interviews (mentioned by 38% of executives).

Businesses also take extra steps to safeguard personal data used by AI systems, such as anonymizing to make it more difficult to trace it back to individuals if it is compromised. At the same time, they are using AI itself to manage security.

AI-powered security is an evolving area—full of potential and caution. Organizations are pensive about the risk involved, with trust being a considerable challenge like in most AI use cases. But the potential gains are huge. For this reason, Rick Kreuser, Lenovo's AI Portfolio Director advises a “risk-forward approach”.

“The AI tools themselves—especially as agents emerge—can be mission-specific, narrow and scalable tools,” he says. “They can quickly and comprehensively do the detection work, as well as portions of the containment, mitigation and remediation work.”

“It remains to be seen how adoption will go,” he continues. “The toolsets present the need for new skills, new safeguards and new levels of complexity—so a risk-forward approach to adoption is advised.”

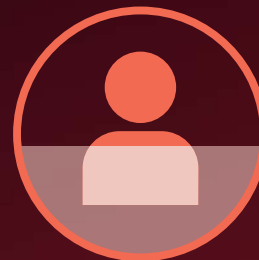
What executives are doing.

Executives are creating even stronger firewalls to keep their infrastructure secure.

“

We’ve set up adequate multi-level firewalls to keep our network safe, monitoring and controlling both incoming and outgoing traffic based on specific security rules, which helps us keep potential threats at bay.”

**CFO,
Financial Services business, India**



38%

More than two thirds of executives mentioned encryption in interviews, as a means to improving AI security.



Reducing AI risks with confidence

Audit and control access.

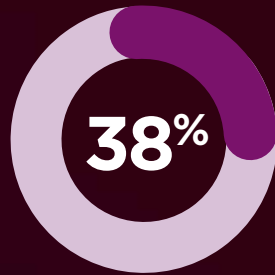
The importance of continual vigilance.

Aligned to the vetting of third-party vendors is a requirement to keep close watch over their AI platforms. Businesses are undertaking internal audits and across partner ecosystems.

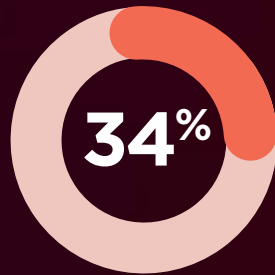
The scope of the audit often depends on the nature of the supplier or offering. It can be light, looking at basics such as ‘purpose’ and whether it is being fulfilled. It could also be customer and product owner feedback. However, if an AI application is high risk, customer critical, or faces government or regulatory reporting requirements, audits typically go deeper and are handled as part of the product owner’s mandate.

Businesses also manage permissions so only authorized individuals can access sensitive data and resources—helping minimize breaches and maintain security and integrity.

The gold standard being applied for access control includes multi-factor authentication, supported by biometrics, where every element of the AI system provides authentication based on a robust Role Based Access Control scheme.



of interviewees highlighted audits as a way to overcome AI security challenges.



of interviewees mentioned use of access control and authentication as a way to overcome AI security challenges.

What executives are doing.

Regular checks are a priority.

“

We implement periodic inspection checks to keep the information contained in them safe from external threats.”

**IT Director,
Hospitality business, France**

“

We’re adopting a zero-trust architecture to keep a close eye on interactions with our AI systems, regardless of where you are or what device a person is currently using.”

**IT Director,
Manufacturing business, USA**

Zero-trust protocols are a popular choice among interviewees.

Reducing AI risks with confidence

Train staff and AI models on security risks.

The strongest defenses combine people and AI working together.

Almost a quarter of interviewees (21%) highlighted the importance of employee training for awareness of AI-related security risks. Training ensures staff know how to identify issues and react appropriately. Training itself might range from a general session on risk identification to more detailed cyber awareness workshops.

All company employees should be trained on the corporate security policy and how it's operationalized. They also need to know what's expected of them regarding threat detection, reporting and follow up. Additional training should be tailored according to security policy, risk tolerance, end-user roles and needs. Throughout, clear guidance is vital, including dos and don'ts, best practices, reference materials and where to go for help.

What executives are doing.

Keeping data safe during downtime is key.

“

We have cyber security awareness and training programs in place to make our employees aware about how they can recognize and respond to emerging cyber threats successfully.”

**Director of IT,
Retail business, USA**

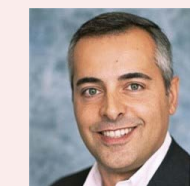
Training AI to counter adversarial attacks.

Adversarial AI—when people trick AI systems into making mistakes by slightly changing the inputs they receive—demands models themselves to receive additional training. By exposing AI models to intentionally crafted, malicious inputs—called adversarial examples—they can learn to identify and handle such inputs, making them less susceptible to future attacks.

Humans also need to be closely involved in vetting outputs. As Lenovo's AI Portfolio Director, Rick Kreuser, puts it: “Take an imperfect AI model and have it judged or governed by an imperfect model, and you've got every chance for things to go sideways. Key in the training is the ‘human in the loop’ aspect—not only looking for what happened in the original model, but also how the adversarial model interpreted it and what it recommended. The training should root itself in the purpose of the model as the north star and humans given transparent and explainable data and pathways to judge.”

“

All employees should be trained on the corporate security policy, its operationalization, and expectations for detection, reporting, and follow-up. Include clear guidance on do's and don'ts, best practices, reference materials, and where to seek help.”



Tiago Da Costa Silva,
Strategy Director, Lenovo
Digital Workplace Solutions

Lenovo



Reducing AI risks with confidence

Create governance against bias.

The importance of inclusivity.

To ensure fairness and eliminate bias, ethical AI and security must go hand in hand. Embedding values means taking an inclusive approach. In our survey, the metric with the highest score was the involvement of diverse demographics, disciplines and experience levels in AI solution development, with 79% of respondents reporting high/very high effectiveness.

Similarly, involving people in the design, development and deployment of AI systems is a high confidence area, with 75% reporting high/very high preparedness.

But issues persist around bias. This can be controlled with a bias-detection set of queries or prompts, or by using people (or a ‘model judging AI’) to inspect the input and output logs.

Develop an internal governance framework.

The extent to which ethical AI policies are formalized is weak.



One way organizations address the weakness of formalizing policies is to develop an internal governance framework to ensure secure and ethical use of AI.

As Tiago Da Costa Silva, Strategy Director, Lenovo Digital Workplace Solutions, comments: “At Lenovo, our Responsible AI policy is very clear on what we should and should not be doing, and the position it occupies in our ecosystem. There’s not one size that fits all, but because of the experience that we have internally, we can help customers as part of their AI journey.”

By way of example, Lenovo’s own Responsible AI framework includes these questions:

Did you consider the impact of the AI system on the right to privacy?

Have you audited your AI system for cybersecurity risk?

Did you define the risks, risk metrics and risk levels of the AI system?



What executives are doing.

Organizations are driving awareness of bias.

“

One major challenge of employing AI is avoiding bias and ensuring fairness. AI systems can unintentionally reinforce or may increase the biases in training data, which may lead to unfair treatment of certain groups. This can cause discrimination in areas like hiring, lending and law enforcement.”

**Director of Finance,
Financial Services business, Argentina**

Organizations are creating teams dedicated to AI governance.

“

We have established an AI governance team within our organization to oversee the secure and ethical use of AI tools.”

**VP Marketing,
Retail business, India**



Lenovo

Key actions.

How to make sure your security is fit for AI.



Anticipate

Understand your starting point.

Know the risks associated with your implementation and benchmark your security readiness using Lenovo's AI Readiness Assessment.

Define your risk appetite.

Establishing your comfort level dictates how deep you'll go, the areas to emphasize, review frequency, resources and the budget.

Audit your AI supply chain.

Take a zero-trust approach to third-party vendors and supply chain partners, implementing regular audits and testing—don't just assume everything is OK.



Secure

Protect data.

Implement layered defenses, including encryption, multi-level firewalls and real-time monitoring to safeguard data.

Control access.

Enforce strict access controls, including multi-factor authentication and robust role-based access.

Engage experts.

AI is new, fast-moving and highly specialized. Work with a trusted partner that delivers AI-specific risk management.



Govern

Create frameworks.

Build internal governance and set the direction for secure and ethical AI use, focusing on eliminating bias and ensuring fairness in your AI systems.

Detect and control bias.

Use bias-detection queries and human oversight to inspect AI input-output logs to proactively address bias and discrimination.

Train and educate.

Invest in employee training on AI-related security risks and adversarial AI defense to ensure staff can effectively identify and mitigate potential threats.



Ready to unleash AI?

Read the rest of the Lenovo AI Readiness Index Series 2025: Technology, People and Processes and learn how Lenovo can help you minimize risk across your AI [here](#).

Discover more AI trends in the [Lenovo Global CIO Playbook 2025](#).

The vision is yours. Get there with Lenovo.

Research methodology



5,000
senior business leaders (C-suite,
VP/Directors, and Senior Managers)



40 global business
and IT leaders interviewed in
November–December 2024



20 countries
in NAMER, LATAM, EMEA,
and APAC in November 2024

Smarter
technology
for all

Lenovo